UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SURGICAL INSTRUMENT SERVICE COMPANY, INC. Plaintiff/Counter-Defendant	) Civil Action No.:) 3:21-cv-03496-VC
Vs.	)
INTUITIVE SURGICAL, INC., Defendant/Counterclaimant	)

HIGHLY CONFIDENTIAL ATTORNEYS' EYES ONLY

Deposition of PAUL D. MARTIN, Ph.D., was taken via videotape and Zoom on Thursday, March 16, 2023, commencing at 10:32 a.m., at 12102 Ashcroft Terrace, Monrovia, Maryland, before MICHELE D. LAMBIE, Notary Public.

Reported By:

Michele D. Lambie, CSR-RPR

APPEARANCES:

ON BEHALF OF THE PLAINTIFF/COUNTER-DEFENDANT:

McCaulley Law Group.

JOSHUA VAN HOVEN, ESQUIRE.

josh@mccaulleylawgroup.com.

3001 Bishop Drive.

Suite 300.

San Ramon, California 94583.

(925) 302-5941

ON BEHALF OF THE DEFENDANT/COUNTERCLAIMANT:

Covington & Burling LLP.

KATHRYN ELIZABETH CAHOY, ESQUIRE.

kcahoy@cov.com.

3000 El Camino Real.

5 Palo Alto Square.

Palo Alto, California 94306.

(650) 632-4700

APPEARANCES CONTINUED:

ON BEHALF OF THE DEFENDANT/COUNTERCLAIMANT:

Covington & Burling LLP.
MIRIAM ARGHAVANI, ESQUIRE.
marghavani@cov.com.
415 Mission Street.
Suite 5400.
San Francisco, California 94105.
(415) 591-7059

ALSO PRESENT: Nolan Church - Videographer
Paul Baker - Concierge

EXAMINATION INDEX

EXHIBITS INDEX
(Attached to Transcript.)

the datasheet up. That's why I'm not super comfortable without doing that. It's always best to do that.

Q. We're -- we're waiting for the internet. Just -- I don't think we need a -- a break though. Just give me a second here as I get this specific document up.

(Brief pause.)

BY MR. VAN HOVEN:

Q. Okay. Who is Atmel?

A. What? I'm sorry, I didn't hear you.

Q. Sorry, yeah. Who is Atmel?

A. They're a company.

Q. What type of company are they?

A. They make chips, generally speaking. At least I know of the chips they make, microcontrollers and other types of chips as well.

Q. And the Dallas DS2505 chip, do you know who makes that chip?

A. So, I'd like to see the data chip for that -- datasheet for that chip, too.

I really prefer to see the datasheets whenever we're talking about chips. There's a lot of room for blending things together otherwise.

Q. Are there a number of suppliers of RFID chips?

A. Yes.

Q. About how many do you think?

A. I could not put an estimate on it.

Q. More than five?

A. Yeah, probably.

Q. Quite a few?

A. Yeah. I mean, I don't know what you mean by quite a few, but there's -- there are -- there are -- I could think of several.

Q. Are there a number of suppliers of wired EEPROM chips?

A. Yes.

Q. More than five?

A. Yes.

Q. Again, quite a few?

MS. CAHOY: Objection to form.

THE WITNESS: The same answer. I'm not sure what you mean by quite a few, but I would say that I'm familiar with many. Like, you know, more than -- more than five certainly suppliers of EEPROM chips I have seen in different examples in my life.

BY MR. VAN HOVEN:

Q. Are RFID chips commodity components?

MS. CAHOY: Objection to form.

THE WITNESS: It depends on your definition of commodity.

BY MR. VAN HOVEN:

Q. There are a lot of suppliers of relatively interchangeable parts with a lot of different specifications?

MS. CAHOY: Objection to form.

THE WITNESS: For certain types of RFID chips, that is true.

BY MR. VAN HOVEN:

Q. What about wired EEPROM chips, are those commodity parts?

A. It's the same answer. So, generally speaking if you're just referring to a generic EEPROM with no other special properties, sure, but, you know, there might be specialized EEPROMS that are -- that have special features, and then they wouldn't be commodity parts. So, it really depends.

You'd have to provide a specific example, but I could say there are many EEPROMS, and many of them are compatible with one another.

Q. I think that I may have beat the internet and get this thing up.

A. Yeah.

(Whereupon, Martin Deposition Exhibit No. 23, Atmel Summary Datasheet, Marked for identification.)

BY MR. VAN HOVEN:

Q. If you could take a look at we've marked as Exhibit 23.

A. I recognize this one, and I am -- yeah, I recognize this one.

Q. Okay. Is -- based on this, do you have an understanding as to whether the Atmel RFID chip used in Xi EndoWrists is an active or passive tag?

A. Yes.

Q. What's your understanding?

A. Wait. This datasheet only has 11 pages.

Q. That's the -- that's the number that you provided me in your report for RFID.

A. Okay. This might be not --

Q. You can go back to the other one that we had, too, if you want.

A. I'll just -- I'll just use the other one. While you were talking, I flipped through it, and it seems to have a lot of the things that I want to refer to for this discussion.

Q. Okay. So, I'll get Exhibit 22 back up, if I can figure out how to do that.

A. Okay. Okay.

Q. Do you have an understanding of whether the Atmel RFID tag used in the Xi EndoWrist is an active or passive tag?

A. I do.

Q. What's your understanding?

A. Sure. Just give me a second to point to where I want to here.

So, if you look under Description in paragraph 2, it describes that the RF interface powers the other circuits; no battery is required.

So, based on how we're using the term in this case, which is a fairly common usage, it's a passive tag. Though, I do note that it's referred to as having an active state, and that's where some confusion can come in, but I would define this as a passive tag.

Q. And -- and so is it your understanding that in the context of a -- of a -- well, okay. Strike that.

An Xi robot, as you understand it, has a reader that is able to interface with the RFID tag in an Xi EndoWrist; is that right?

A. That's my understanding.

Q. And the reader is a device that lights up

the RFID tag via a wireless signal, is that how you understand that to work?

A. That's part of what it does.

Q. Assuming that the RFID reader within the robot arm is -- is providing that signal to light up the tag and the tag is in proximity of the arm, will the -- will the tag light up and respond?

A. It should.

Q. It wouldn't need to be attached to do that, would it?

A. The tag is attached to the arm.

Q. I mean, the arm -- the -- the EndoWrist wouldn't need to be attached to the arm for the tag to respond, assuming the reader is sending a signal?

MS. CAHOY: Objection to form.

THE WITNESS: Oh, I see. The answer is it probably wouldn't, but I could think of a few configurations in which you could design -- design a device where that wouldn't be true necessarily, but it shouldn't.

BY MR. VAN HOVEN:

Q. But -- yeah, absent one of those special kind of configurations, as long as you're within the range of whether it's three inches or six inches, it should light up and activate and respond?

A. With the caveat, I haven't tested this, but it should.

Q. Can we go to -- actually, let's go into something else. What's a -- have you ever heard the term whitelist in the context of information security?

A. Yes.

THE WITNESS: But just to pause. If we're going into something else, depending on how something else, how long it is, it might be a good time for lunch.

MR. VAN HOVEN: Yeah, no. Yeah, you're -- you're getting late into your -- so, yeah. Why don't we take a little break or a longer break.

Mr. Shafer?

A. No.

Q. I'd like to talk a little bit about the use counter on the Xi EndoWrist, okay?

A. Did you say Xi?

Q. Yes, Xi, the -- the more recent generation.

A. Okay. Sure.

Q. And do you understand that the use counter value is stored on the Atmel CryptoRF chip that we've been discussing within an Xi EndoWrist?

A. Yes.

Q. Do you know if that use counter value is stored at a kind of particular region of memory within the Atmel CryptoRF chip?

A. It is stored within a particular region of memory.

Q. Do you have an understanding as to whether that region of memory is read only?

A. Give me one second, please.

(Whereupon, there was a pause for

document examination.)

THE WITNESS: I'm still examining parts of the report, so please just give me a little bit more time.

BY MR. VAN HOVEN:

Q. No problem.

(Whereupon, there was a pause for document examination.)

THE WITNESS: Okay. Apologies still. Because there's no search, it's taking me just a little bit longer.

(Whereupon, there was a pause for document examination.)

THE WITNESS: Okay. Now, can you please ask your question again?

BY MR. VAN HOVEN:

Q. Do you have an understanding as to whether that region of memory that includes the use counter value is read only?

A. So, it depends what you mean by read only, but at the very least, that region of memory

hypothetical because there are external questions that need to be resolved to answer it.

BY MR. VAN HOVEN:

Q. You do understand that my question is limited to the Atmel CryptoRF chip as implemented in Xi EndoWrist, correct?

A. I understand that much.

Q. Is the CryptoRF chip programmable once it's, I guess, out in the field in an Xi EndoWrist to your knowledge?

MS. CAHOY: Objection to form.

THE WITNESS: It depends what you mean by programmable.

BY MR. VAN HOVEN:

Q. Sure. Can values stored in memory of the CryptoRF chip be changed in the field when implemented in an Xi EndoWrist to your knowledge?

A. Sure. So, for instance, values can be decremented.

Q. Any other types of changes? Can other values be changed in an Atmel CryptoRF chip?

A. I don't know.
Q. Do you know if --
A. But hold on.
Q. Sure.
A. In the context of the EndoWrist Xi, I don't know. In the context of a CryptoRF chip in a vacuum, there are various things you can do to the chip as -- as specified in the datasheet.
Q. Including changing values that have previously been programmed into the chip; is that right?
MS. CAHOY: Objection to form.
THE WITNESS: Well, the chip has like a whole bunch of different features. It really depends on how the chip has been -- like what the actual design of your system is.
BY MR. VAN HOVEN:
Q. But one possibility with the CryptoRF chip is that you can change values that have previously been written -- written on to the chip, right?

MS. CAHOY: Objection to form.

BY MR. VAN HOVEN:

Q. That's something that's possible?

A. You would need to have a system set up to allow for that.

Q. Is the -- to your knowledge, is the use counter value that's stored on a CryptoRF chip in an Xi EndoWrist, is that value stored in -- in an encrypted form?

A. My understanding is that -- you said on an EndoWrist X/Xi. My understanding is that that value along with some other values are encrypted on that -- on those devices.

Q. What type of encryption is used for that?

(Whereupon, there was a pause for document examination.)

THE WITNESS: I don't think that's entirely clear from what I have seen.

BY MR. VAN HOVEN:

Q. So, you don't know what type of encryption is used for the use counter on the Xi

EndoWrist; is that right?

A. I think that's right. The evidence that I have seen has been conflicting on that front and in one case incorrectly referenced SHA as a type of encryption.

Q. But you don't personally know what type of encryption is used for the use counter on the Xi EndoWrist, right?

A. I don't believe I know all of the specifics of the cryptography used to encrypt the use counter and other information on the CryptoRF chips.

Q. What specifics do you know of the cryptography -- cryptography used to encrypt the use counter on the Xi EndoWrists?

A. I know the information in the datasheet about various things that are supported with respect to cryptography on these chips.

Q. But you don't know what Intuitive uses within that datasheet?

A. I don't know what they ultimately

selected.

Q. If you were tasked to attempt to circumvent the encryption of the use counter on the Xi EndoWrist, how would you go about that?

MS. CAHOY: Objection to form.

THE WITNESS: Oh, that's like a really complicated question. I don't think I could -- that's an entire like work engagement. That would take a lot of analysis just to figure out how to even approach the problem.

BY MR. VAN HOVEN:

Q. But let's just assume that you have access to the Atmel CryptoRF chip that has a use counter value on it that is encrypted, okay?

A. Okay.

Q. In that, you can either physically or wirelessly communicate with the chip?

A. Okay.

Q. And that you have the datasheet that tells you the types of encryption that's implemented, --

A. Um-hum.
Q. -- right? And you -- you have that datasheet, right?
A. Yes.
Q. So, given that information based on your 15 to 20 years of information security experience, as a general approach, how would you go about trying to circumvent the encryption on the use counter within an Atmel CryptoRF chip?
A. So, I -- I just haven't done that analysis.
Q. I understand. I'm -- but you're here to testify as an expert in the area of information security and I just want to understand the general approach you would take.
MS. CAHOY: Objection to form.
THE WITNESS: Right. So, the problem is it's a specific problem for a specific chip, and I would need to do a good amount of legwork to figure out what that approach would be. I haven't done that legwork, so I don't know what my approach

would be.

BY MR. VAN HOVEN:

Q. What type of legwork is typically involved in trying to attack that sort of problem?

A. I would need to spend some time thinking about it.

Q. So, time is one piece of -- one part of that legwork?

A. I don't think time is what I would call part of any legwork. Time is just a resource that you need to have to do anything.

In the absence of any time at all, everything would stand still, right? So, it's not clear what that means.

Q. I'm not talking about us getting close to the speed of light or anything here, but I'm just trying to understand, you said that there would be legwork. And I'm just trying to, what is -- what is the kind of legwork that -- that you're envisioning to attack the problem of circumventing the encryption as we've described on the Atmel

CryptoRF chip?

A. Sure. So, the -- the truth is that's -- that's complicated, and I haven't really thought about it.

Q. But you'd have to think about it a little bit, right?

A. Yes, I would have to think about that.

Q. You'd have to look at the datasheet?

A. Certainly, looking at the datasheet would be a part of any legwork.

Q. You would have to --

A. That would be true.

Q. Excuse me. You would have to perform some sort of direct electrical or in -- indirect communication channel probing of the chip probably?

MS. CAHOY: Objection to form.

THE WITNESS: At -- at some stage in the process, you would need to connect to the chip, but I haven't really thought about when or how that would occur. So, I don't have any more insight into that.

BY MR. VAN HOVEN:

Q. Do you think that the encryption employed by the CryptoRF chip is particularly complicated compared to the sort of encryption you typically have worked with?

A. I don't have an opinion on that.

Q. You don't know one way or the other?

A. I would need to investigate it more to figure it out.

Q. And you understand or do you have an understanding that, that the use counter value at some point is transmitted from the EndoWrist to the robot?

A. Yes.

Q. Do you know if that value is transmitted in that encrypted form or if it's decrypted before it's transmitted?

A. I understand the value to be encrypted when it's transmitted.

Q. What's the basis of that understanding?

A. My understanding is from the datasheet

counting data areas of the RFID tag are one-time programmable.

That means they can be -- not be modified once written. Though, of course, they could be decremented, which is an important point.

And so it reads to me that Intuitive documents state that the data is encrypted both at rest and in motion.

BY MR. VAN HOVEN:

Q. And your opinion in that regard is based solely on those documents, right?

MS. CAHOY: Objection to form.

THE WITNESS: I can also see that the datasheet supports those configurations.

BY MR. VAN HOVEN:

Q. As far as the encryption while the -- and here I'm talking specifically about the communications between the Xi EndoWrist and the Xi robot.

As far as the encryption while the data is at motion -- in motion, what would be your

approach to try -- if you were trying to circumvent that encryption?

A. Well, that's -- again, that's sort of the same problem as trying to reverse engineer or break the chip and -- as whole, right?

If I could circumvent that communication, then I would know how -- if I knew how to do that, I would know how to break the communication protocol, so it's the same issue. I don't -- I haven't performed that analysis. I don't know.

Q. But -- but that is your -- your primary area of expertise and study over the last 20 years, right?

A. Yes, I've done many of these. They always require a very thorough set of, you know, thoughts and research and legwork before you can really come up with an approach, and I haven't done that. I haven't done that part of what my normal practice would be.

Q. Yeah. So, if you were to approach a problem like this in your normal practice, what

sort of legwork would you need to perform?

A. Right. So, I would need to look at the individual issues at play, and I would need to look at the product and how it's designed. Let me just think about it and come up with an approach, and that would kind of let me determine what legwork I need to do to then -- so, I would need to think about what I would need to know. Then I would need to think about from what I needed to know, I would know that -- learn that information and figure out from that what I would do to attack.

So, it's a multi-step process, and I haven't performed even the first step yet is the problem.

Q. You just haven't examined that for the Xi EndoWrist, right?

A. That's right. Yeah, I haven't performed an analysis of what would be required to break the device.

I reviewed Mr. Humphrey's analysis. I saw that wouldn't work, but I haven't performed an

Q. And so in your role kind of as a manager at Harbor Labs, are you involved in like providing quotes or estimates to -- to customers who ask you to do something like that?

A. Sometimes. I don't typically do the medical quotes.

Q. Okay. When -- when you're involved in -- in quoting one of these security-based activities, what -- what type of process do you undergo typically?

A. So, when drafting a quote, you -- you usually are going to get a sense of how many components are in the system, the complexity, the amount of code. You're going to look at the programming languages that are used, how old the design is, possibly information about its architecture. You're going to get information about design docs and manuals, but not just external ones, internal ones, and especially requirements documents and other internal information.

You'll study that, which is already a decent amount of work, and then you'll write a quote. Usually, you'll create an MSA and a SOW.

So, you'll write into your SOW at least enough to recover that initial legwork plus the, you know, amount to cover what you think the product is.

To be honest, it's a pretty tricky business providing an accurate quote. It seems that we tend to underquote quite a lot in -- in our work.

Q. Sometimes you -- you kind of use more -- end up using more time and resources than you originally quoted?

A. Because it's so inexact, you don't know how hard it is to perform a particular task until you start working on it. Things might not work in exactly the way you anticipated, and that's why legwork is so important. The more legwork you do, the more accurate your quote will be.

MR. VAN HOVEN: Okay. Dr. Martin, I